

Git Credentials in AIQ

Recommended guidance

Use Git credentials in AIQ only for approved repository access. Credentials should be scoped, rotated, and stored through approved mechanisms instead of being copied into scenario steps, documentation, logs, or shared screenshots.

Credential options

- Personal access tokens or service-account tokens approved for automation.
- SSH keys managed by the repository owner or platform team.
- Read-only access when AIQ only needs to pull repository content.
- Write access only when the workflow explicitly requires AIQ to push changes.

Security checklist

1. Confirm the repository, branch, project, and required access level.
2. Use least privilege and avoid broad organization-level access.
3. Document owner, expiration, rotation, and revocation process.
4. Test repository connectivity without exposing the credential value.
5. Remove old credentials when users leave or repository ownership changes.

Last updated: October 6, 2026

Revision #4

Created 2026-07-31 16:28:57 UTC by Admin

Updated 2026-10-06 18:19:00 UTC by mmora